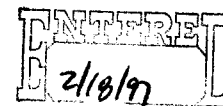


ALSTON & BIRD

601 Pennsylvania Avenue, N.W.
North Building, Suite 250
Washington, D.C. 20004-2601

202-508-3300
Fax: 202-508-3333



Thomas E. Crocker

Direct Dial: 202-508-3318

February 13, 1997

By Hand Delivery

Nancy Crowe
Regulatory Policy Division
Bureau of Export Administration
Room 2705
Department of Commerce
14th Street and Pennsylvania Avenue N. W.
Washington, D.C. 20230

Re: Comment on Bureau of Export Administration Interim Rule on Encryption Exports (61 Federal Register 68572 (December 30, 1997))

Dear Ms. Crowe:

I hereby submit written comments on the above interim rule (the "Interim Rule"). These comments are submitted solely on my own behalf as an attorney with over 20 years experience in the export control area. They draw on my background as a former Department of State official and as the author of portions of the International Traffic in Arms Regulations. However, the views expressed herein are strictly my own and do not represent the position of any particular client, Alston & Bird or the Department of State.

1. Truth in Rulemaking

I commend the Bureau of Export Administration for its effort to achieve a balance in the Interim Rule between the concerns of the national security and law enforcement communities on the one hand and the realities of a rapidly changing market place on the other hand. This largely thankless task is essential to the operation of good government.

Notwithstanding this laudable goal, I must express some concern about the presentation of the Interim Rule to the industry and the public. In announcing the initiative on October 1, 1996 which culminated in the Interim Rule the Vice President stated that the key recovery strategy that the Interim Rule implements must be "industry-led" and that the "ultimate solution must be market-driven." The problem is that the Interim Rule is neither. It not only mandates detailed criteria for key recovery agents but also establishes

extensive Commerce Department approval and oversight over them. It even mandates the time frame within which agents must respond to key requests (two hours). This rulemaking is not an industry-led or market-driven solution. Commerce is well aware that the "key management infrastructure" ("KMI") is an unproven technology for which there is as yet no market. Moreover, but for the Interim Rule there would be no market. Similarly, the major U.S. allies in the Organization for Economic Cooperation and Development ("OECD") have declined to endorse KMI. This is not to say that KMI should not be adopted. However, it is to say that the Administration's credibility and good faith in advancing this proposal are harmed by portraying it as something it is not. The Administration should drop all pretenses and call the Interim Rule what it in fact is: a government-imposed solution with limited input from the private sector.

2. Additional Thought to and Minimalization of Mandatory Criteria

Alternatively, the Administration could drastically scale back the detailed criteria and oversight spelled out in Supplements Number 4 through 7 to Part 742 (especially the 27 criteria of Supplement Number 5 regarding key recovery agents) under the Interim Rule in order to allow for true industry-led development of KMI. This approach may be preferable, and indeed only prudent, in light of the unproven technology that KMI demands. For example, how does Commerce know that a two-hour response time will work, especially with regard to systems, such as Netscape's, which produce unique session keys which could run into the billions as encrypted transactions proliferate?

In addition, I have a concern that the 27 criteria of Supplement Number 5 are at once inadequate to ensure true security and too intrusive to allow for a market-driven KMI industry. This paradox is reflected in the fact that the entire Commerce-mandated system is based on representations of the identity of personnel involved in KMI. Anyone with minimal criminal or espionage experience, much less a sophisticated foreign operative, could circumvent these procedures and gain access to keys. This vulnerability is compounded by the shotgun approach of potentially allowing virtually any entity to qualify as a key recovery agent, thereby providing a multitude of points of entry for wrongdoers. Policing this universe of recovery agents will be difficult, if not impossible. Security breaches are likely to occur. Arguably, security might be better ensured by the concentration of all recovery agency operations in a few proven institutions or a sector, such as banks or other entities. More thought needs to be given to this problem.

Related to this problem, as well as to the milestones (six-month reviews, etc. involved in seeking approval for export of strong encryption (discussed further below)), is the tendency to favor large sophisticated exporters. As experience with the self-compliance requirements of the Distribution License under the Export Administration

Regulations has shown, small to medium-sized companies find this type of exercise costly, obtuse and generally infeasible. Perhaps this is Commerce's intent after all. If so, why purport to open recovery agency up to potentially any applicant? Does Commerce really want a widely diffused and accessible KMI or does it want market forces to concentrate KMI in a few large entities? This is not to imply that this course is wrong. It may be right. It is just not clear what the game plan is.

Coupled with these potentially weak security controls in the Interim Rule is a paradoxically intrusive scheme of paperwork, recordkeeping, reporting and approvals, all directed to the Commerce Department. Basically, it is little more than a government paperwork exercise that has no proven assurance of providing the security that it purports to seek.

3. Need for Greater Procedural Transparency

On a more practical level, the Interim Rule needs to be revised to provide greater transparency in its operation. It is simply not clear how it operates, what the distinctions are between the categories of encryption it addresses, what procedures applicants must follow to get export approval or what kind of documentation they must submit or to whom. The following examples are illustrative only, and the entire document should be carefully reviewed in order to improve its procedural clarity.

i. Section 740.8 (b)(1) covers "recovery encryption software and equipment" without defining what it is. Is this software and equipment that implements KMI or is it encryption product that is subject to KMI? Or is it simply another way of saying public key? What exactly does Commerce mean to cover in this category?

ii. The same questions apply to the undefined term "non-recoverable encryption items" at Section 740.8 (b)(2). The language of this section appears to suggest that this category is limited to 56-bit DES. Is this another way of saying private key? What is the exact delineation between subsection (b)(1) and (2) products? Where does one leave off and the other pick up?

iii. Assuming there is a difference, why does a subsection (b)(1) application have to be supported by full-scope Supplement Number 4 and 5 criteria, while a subsection (b)(2) application needs only be supported by a Supplement No. 7 plan showing how the applicant intends to move toward

KMI? In other words, if they are different, why must they both support KMI but with different documentation? There may be a good reason, but it is not clear.

iv. Similarly, Commerce states at Section 742.15(b)(2), with specific reference to subsection (b)(1) products, that "Since the establishment of a key management infrastructure and key recovery agents may take some time, BXA will, while the infrastructure is being built, consider exports of key recovery encryption products which facilitate establishment of the key management infrastructure before a key recovery agent is named," subject to certain conditions. What is the difference between this and the (b)(2) category where it is a non-recovery item? Why doesn't an applicant have to submit a Supplement Number 7 plan under these circumstances? Again, what are the precise distinctions between these items?

v. The fourth category of product at Section 742.15(b)(4) appears to be a basket category for case by case licensing of products that do not qualify for the KMI exception. Separate conversations with Commerce licensing staff suggest that Commerce may use this provision to approve export of encryption even stronger than 56 bits, especially for financial services applications. However, this is not clear from the Interim Rule, and it should be clarified that Commerce's intent is to preserve the financial services exception if this in fact is the case. Once again, it is not clear from the Interim Rule what Commerce is doing.

vi. The descriptions of who can apply for and rely upon a one-time classification are unclear and contradictory. Thus, Section 742.15(b)(3) states that "manufacturers" are permitted to export under License Exception KMI but that "exporters" must submit the classification request. What happens if the manufacturer is not the exporter? Who must do what then? The same section further on states that BXA will accept requests for classification from distributors, re-sellers, integrators and other entities that are not manufacturers. This seemingly contradicts the above language. Moreover, the Interim Rule also confusingly states that entities that are not manufacturers are permitted to use License Exception KMI only if a classification has been granted to the manufacturer and that the time period of the authority for export of the item will be determined by the time period applicable to the manufacturer's authority to export. In short, who must apply and who can rely on the ruling? In this connection, suppose a

manufacturer develops a product for use in the financial services industry. Does approval have to be obtained for the generic product only or (as required by the State Department up to now) for the product as incorporated into the specific bank's program, in which case the bank would presumably be part of the review process? How else can Commerce vet the product as applied in practice? Has it concluded that this is no longer necessary?

vii. The documentation that must be submitted to obtain eligibility for License Exception KMI is not spelled out in the Interim Rule. If Form BXA 748P is implicitly required, this should be made explicit. Similarly, the Interim Rule contains insufficient guidance on how an applicant should format and describe the information required by Supplements Number 4 and 5 and, especially, 7. Based on the wording of the Interim Regulation, it is virtually impossible to guess what Commerce wants in the way of a business plan to satisfy Supplement Number 7. If these criteria are not clear from the regulation, should the applicant request a pre-application conference with Commerce staff and, if so, with whom?

4. Deemed Export Rule

The Interim Rule makes a potentially significant liberalization in terms of the definition of "export." Under Section 734.2(b)(9), a special definition of "export" applies to exports of encryption source and object code software. Thus, the export of such software is limited to an "actual shipment, transfer or transmission out of the United States" or the "transfer of such software in the United States to an Embassy or affiliate of a foreign country." "Export" therefore does not cover the release of software to a foreign national in the United States (other than an Embassy or foreign country affiliate), such as a foreign national computer programmer. The deemed export rule thus does not apply to encryption software under the Interim Rule. However, Commerce staff continue to advise the public that it does apply, notwithstanding the absolutely clear language of the definition. This issue should be resolved or clarified.

Moreover, even if the deemed export rule were no longer to apply to encryption software under the above definition, it would appear to continue to apply to encryption equipment and technology. It is unclear why Commerce carved out an exception only for encryption software but not equipment or technology. This also should be clarified.

5. Uniquely Restricted Treatment of Encryption

In addition, there are a number of instances in the Interim Rule where provisions of the Export Administration regulations which are normally applicable do not apply in the case of encryption products. Thus, encryption items are not subject to mandatory foreign availability procedures, and controlled encryption software will remain subject to control even when it is publicly available (unlike other software and technical data under the Export Administration Regulations). There is no coherent explanation in the Interim Regulations as to why this should be the case, other than the fact that these limitations were contained in Executive Order 13026. This exceptional treatment should be fully explained and justified beyond vague reasons of "national security."

6. Encryption Technology

Under the Interim Rule Commerce will consider applications for export and reexport of encryption technology (presumably covering training and MRO assistance) covered by ECCN 5E002 only on a case by case basis. Encryption technology seemingly will not be eligible for License Exception KMI and the more liberal treatment afforded encryption products and software. The reason for this differing treatment is unclear. Because exports of encryption products frequently may involve related transfers of technology this specific licensing requirement may be a significant stumbling block to use of the other supposedly liberalized export control procedures contained elsewhere in the Interim Rule.

7. Level Playing Field

If the other OECD countries do not adopt KMI but U.S. companies only are subject to it, this raises a level playing field issue that Commerce can hardly ignore. The experience with the abolition of COCOM in 1994 is instructive. At that time, by abolishing the single member veto but retaining unilateral U.S. export controls, the Administration put U.S. exporters in the unenviable position of potentially having to compete with their counterparties from the former COCOM countries at a disadvantage. Although the Administration eventually took steps to rectify this disparity, it was only after a number of commentators (including the author of this comment letter) pointed the problem out publicly that the Administration thought through and recognized the issue. This should not happen again. Unless there is discernible and prompt movement toward multilateral agreement on KMI U.S. exporters should not be disadvantaged.

8. Liability Issues

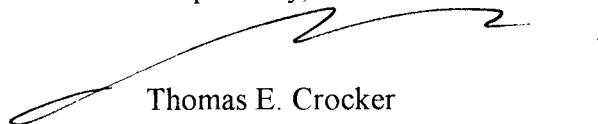
Commerce appears to recognize that legislation will be required to resolve liability issues for key recovery agents. This is unquestionably true if KMI is to stand a chance of market acceptance. The Administration should move quickly to develop and enact such legislation. However, in so doing, it should consult more thoroughly with industry than it appears to have done in developing the Interim Rule in order to avoid a flawed, government-imposed product that does not address all concerns. The Administration should place high priority on this issue.

9. Resources

Finally, because of the burdens and confusion associated with Commerce's new encryption responsibilities, the Administration and Congress should ensure that Commerce has adequate staffing to be responsive to the public and process licenses in an expeditious manner. Recent experience with STELLA and licensing officers responsible for encryption (e.g., waiting an hour and a half to get through and five successive calls in ten days not returned) suggests that there may be a problem reminiscent of the bad old days of the mid-1980s. Commerce should nip this problem in the bud if it wants this program to be a success, and the Administration and Congress owe it to Commerce to give it the resources it needs to do so.

In conclusion, the above comments, while in certain instances critical, are proffered with a constructive intent to help Commerce implement a successful program.

Respectfully,

A handwritten signature in black ink, appearing to read 'Thomas E. Crocker', with a long, sweeping horizontal stroke extending to the left.

Thomas E. Crocker

TEC:caf

DC970440023